

Subject: [EXTERNAL] ATTORNEY GENERAL WILLIAM P. BARR DELIVERS REMARKS AT THE LAWFUL ACCESS SUMMIT

Date: Friday, October 4, 2019 at 11:21:41 AM Pacific Daylight Time

From: USDOJ-Office of Public Affairs

To: Farivar, Cyrus (NBCUniversal)

seal - centered header for gov delivery

The United States Department of Justice

FOR IMMEDIATE RELEASE

FRIDAY, OCTOBER 4, 2019

WWW.JUSTICE.GOV/NEWS

ATTORNEY GENERAL WILLIAM P. BARR DELIVERS REMARKS AT THE LAWFUL ACCESS SUMMIT

Remarks as Prepared for Delivery

Washington, D.C.

Thank you for that introduction.

It's great to see so many members of the law enforcement community here today. Many of you have come from far away, and we are grateful for your presence. You are joined by those from the NGO community, industry, academia, and Capitol Hill. This is likely the first time that so many stakeholders in the lawful access conversation have been in one place.

I'm especially thankful to be joined by two good friends from abroad: Peter Dutton, the Australian Minister for Home Affairs, and Priti Patel, the U.K. Home Secretary. Thank you to each of you for accepting my invitation to be here, and for traveling such a long way. Our nations face a constellation of common security concerns. But we do not face them alone. We have always stood shoulder to shoulder in the fight for freedom, peace, and security. And we will continue to do so.

Just last night, Priti and I, on behalf of our governments, signed the first-ever agreement under the CLOUD Act, which became law last year thanks to industry support, bipartisan Congressional action, and President Trump's leadership. That Act greatly facilitates criminal investigations by allowing law enforcement from each country to obtain evidence directly from commercial providers pursuant to legal process that safeguards privacy rights.

The theme of today's summit – warrant-proof encryption – is distinct from the CLOUD Act. But the Act is worth mentioning at the outset because it serves as an excellent example of how much we can achieve when all stakeholders come together in pursuit of a common goal. To address the lawful access issue, it will take that kind of commitment, along with an honest, public discussion of pros and cons.

As individuals and as a nation we have become dependent on a vast digital infrastructure.

That, in turn, has made us vulnerable to cybercriminals and foreign adversaries that target that infrastructure. Encryption provides enormous benefits to society by enabling secure communications, data storage, and online transactions.

As the Federal Government, we welcome these improvements to privacy and security, and will work to preserve and strengthen them.

But the digital world that has proven such a boon in many ways has also empowered criminals. Like everybody else, criminals of all stripes increasingly rely on wireless communications, hand-held devices, and the internet. In today's world, evidence of crime is increasingly digital evidence. As we work to secure our data and communications from hackers, we must recognize that our citizens face a far broader array of threats. Hackers are a danger, but so are violent criminals, terrorists, drug traffickers, human traffickers, fraudsters, and sexual predators. While we should not hesitate to deploy encryption to protect ourselves from cybercriminals, this should not be done in a way that eviscerates society's ability to defend itself against other types of criminal threats. In other words, making our virtual world more secure should not come at the expense of making us more vulnerable in the real world.

Enjoyment of all the personal rights we cherish – whether to life, liberty, property, speech, or privacy – ultimately depends upon our ability to maintain a safe society. Whether you agree with John Locke about everything, he was certainly right about that. The founding document of our republic, the Constitution, states at the outset that one of the principal reasons we have framed our body politic is to provide this security – “to provide for the Common Defense,” that is, security from foreign enemies; and “to insure Domestic Tranquility,” that is protection from the predators within our society. Unless society as a whole has the ability to preserve this peace and security, our rights ultimately become meaningless.

The essence of all political thinking is about how we reconcile the claims of the individual with the interests of the broader community. In all the great countries represented on the stage, we have erected strong protections around our individual rights, while at the same time placing some constraints on them where necessary to protect the safety of society as a whole.

Apart from life itself, liberty is our greatest value. And yet, limits are placed even on this core right when necessary to protect society. We deprive people of their liberty – we arrest them – when we have probable cause to believe they have committed, or are engaged in, a crime.

If we could wave a magic wand and conjure up a technology that could enhance our liberty by absolutely insulating every individual from being hindered – even preventing any possibility of arrest – would we want to deploy it? It might protect the innocent from muggers but it would also insulate all criminals from arrest.

What is happening here is that some companies want to say to the individual, “Hey, we can make you invisible to law enforcement.” But do we want to live in a society where everyone is invisible to law enforcement?

These considerations apply to privacy. That right has never been absolute. The Fourth Amendment strikes a balance between the individual citizen's interest in conducting certain affairs in private and the general public's interest in subjecting possible criminal activity to investigation. It does so, on the one hand, by securing for each individual a private enclave around his “person, house, papers, and effects” – a “zone” bounded by the individual's own reasonable expectations of privacy. So long as the individual acts within this “zone of privacy,” his activities are shielded from unreasonable Government investigation.

On the other hand, the Fourth Amendment establishes that, under certain circumstances, the public has a legitimate need to gain access to an individual's zone of privacy in pursuit of public safety, and it defines the terms under which the Government may obtain that access. When the Government has probable cause to believe that evidence of a crime is within an individual's zone of privacy, the Government is entitled to search for or seize the evidence, and the search usually must be preceded by a judicial determination that "probable cause" exists and be authorized by a warrant.

As you heard this morning, some companies want to deploy end-to-end encryption on consumer products that would completely prevent law enforcement from gaining access to data or communications, even when there is probable cause to believe a crime is underway and a judicial magistrate has issued a warrant. Essentially, this would establish privacy as an absolute right without any regard to the safety of society as a whole.

It is hard to overstate how perilous this is. By enabling dangerous criminals to cloak their communications and activities behind an essentially impenetrable digital shield, the deployment of warrant-proof encryption is already imposing huge costs on society.

It's not just the reprehensible behavior of sexual predation on children, but myriad additional forms of serious crime enabled by end-to-end encryption. This technology is quickly extinguishing our ability to detect and prevent a wide range of criminal activity – from terrorism, to large-scale drug trafficking, to financial fraud, to human trafficking, to transnational gang activity. The clock is ticking.

One further point about the costs imposed on society by warrant-proof encryption: It is not only about the crimes that could have been avoided, or the criminals that escape punishment. Converting the internet and communication platforms into "law free" zones, and thus giving criminals the means to operate free of lawful scrutiny, will inevitably propel an expansion of criminal activity. If you remove any possibility that the cops are going to be watching a neighborhood, the criminals already in the neighborhood will commit a lot more crimes.

Let me address some of the canards that are floating around in this discussion.

First, it is claimed that law enforcement is asking to impinge on privacy. Nothing can be further from the truth. We are not seeking to move the goal posts at all. We are seeking to preserve the degree of privacy to which we have always been entitled under our Constitution. It is not a degree of privacy that is absolute and impervious under all circumstances. It is a right to privacy that allows for lawful access when society can demonstrate a sufficiently compelling need.

In this regard, I was amused to see the impassioned statement from a leading digital-rights activist two days ago. It said: "A secure messenger [platform] should provide the same amount of privacy as you have in your living room." That is right. I agree. That's exactly what law enforcement is seeking. And as you should all know, with a warrant, law enforcement can gain access to your living room, both physically and virtually.

It is also said that the Government is seeking a secretive "backdoor" to everyone's communications and data. That is false. We are seeking a front door. We would be happy if the companies providing the encryption keep the keys. What we are asking is that some responsible party have the keys so that, when we can demonstrate a lawful basis – probable cause that crimes are being committed – law enforcement is able to gain access.

It also seems to me that the argument of companies that want to deploy warrant-proof encryption rests on an unsustainable premise. The companies seem to think that the debate is over once they show that their technology will achieve some incremental increase in privacy, regardless of its impact on the welfare of society. But, as our whole history shows, the extent of rights has always depended on a balance between the claims of the individual and the claims of society as a whole.

Think of it this way. In the hierarchy of rights and values, the right to life is at the top. There are many technologies available that could provide more security for my personal right to life. I'd be much safer cruising down the highway in an M1 tank. But the risks that would be invariably posed to all the other drivers would be too great. Optimizing for one value, and one value only, is not the end of the inquiry. The externalities of achieving that isolated goal at all costs are just unacceptably high.

The heart of the matter is this: Do the security advantages of warrant-proof encryption offered to the individual outweigh the risk posed to the public by that same technology? This is not a decision for the companies to make by themselves. It is a decision for society to make.

The public can enjoy the benefits of encryption while still allowing for lawful access. There's no doubt that we all benefit from encryption. It allows for e-commerce and many other online applications. But those aren't the applications we're talking about. We are not talking about consumers' interactions with online enterprises, such as banks and retailers. Law enforcement can go to banks and firms dealing with customers and request and receive access to information with a warrant. Nor are we talking about the encryption that enterprises, like power companies, use to protect their operations. What we're instead concerned about is consumer-to-consumer communications, consumer devices, and data storage.

The argument is made that, to achieve perfect protection against bad actors, it is essential to override society's interest in retaining lawful access. Some hold this view dogmatically, claiming that it is technologically impossible to provide lawful access without weakening security against unlawful access. But, in the world of cybersecurity, we do not deal in absolute guarantees but in relative risks. All systems fall short of optimality and have some residual risk of vulnerability – a point which the tech community acknowledges when they propose that law enforcement can satisfy its requirements by exploiting vulnerabilities in their products. The real question is whether the residual risk of vulnerability resulting from incorporating a lawful access mechanism is materially greater than those already in the unmodified product. The Department does not believe this can be demonstrated.

We are confident that there are technical solutions that will allow lawful access without materially weakening the security provided by encryption. Such encryption regimes already exist. To that point, the tech community regularly implements new features that slightly affect the potency of encryption and other security protocols. They do so because it's profitable and those features benefit consumers. For example, providers design their products to allow access for software updates using centrally-managed security keys.

Moreover, even if allowing for lawful access resulted, in theory, in a slight risk differential, its significance should not be judged solely by the fact it falls short of theoretical optimality. The significance of any incremental risk should be assessed based on its practical effect on consumer cybersecurity, as well as its relation to the net risks that offering the product poses for society. And the analysis must take into account alternative and less socially injurious ways of mitigating the risk.

If one already has an effective level of security – say, by way of illustration, one that protects against 99 percent of foreseeable threats – is it reasonable to incur massive further costs to move slightly closer to optimality and attain a 99.5-percent level of protection, even where the risk addressed is extremely remote? A company would not make that expenditure – nor should society.

At the end of the day, we must make these choices based on the net benefit to society. If the choice is between a world where we can achieve a 99-percent assurance against cyber threats to consumers, while still providing law enforcement 80 percent of the access it might seek; or a world, where we have boosted our cybersecurity to 99.5 percent but at a cost reducing law enforcements access to zero percent – the choice for society is clear.

I want to make a point about our freedom and our privacy. Throttling the ability of law enforcement to detect and interdict criminal actors does not advance either value.

Ultimately, there are two ways of protecting society: either detect and neutralize the bad guys or regiment society as a whole. Anyone who has gone through a security line at an airport – sometimes removing your shoes, belt, and toiletries for all to see – knows firsthand the burden that regimentation places on privacy rights.

More so than ever before, the principal tool law enforcement has to identify and neutralize the bad guys is to listen to and read their communications. There is no substitute. If we lose the ability to conduct electronic surveillance or to access digital records, we will inevitably be driven to greater and greater regimentation of society in order to secure ourselves. In turn, we will lose our liberty as well as our privacy. That is the extremely high price we will pay if we prioritize impenetrable encryption above all else.

I do wish to give credit where credit is due: Some tech companies have taken significant steps to help detect and report criminality. When it comes to preventing crime, we hope that industry will be an ally, not an adversary. We hope that the power of technology will provide greater safety to the public, not place us at greater risk of harm and exploitation.

We think our tech sector has the ingenuity to develop effective ways to provide secure encryption while also providing secure legal access. It is well past time for some in the tech community to abandon the indefensible posture that a technical solution is not worth exploring, and instead turn their considerable talent and ingenuity to developing products that will reconcile good cybersecurity to the imperative of public safety and national security. As Microsoft's Bill Gates has observed, "[t]here's no question of ability; it's the question of willingness."

Obviously, the Department would like to engage with the private sector in exploring solutions. The time to achieve that may be limited. As this debate has dragged on, and deployment of warrant-proof encryption has accelerated, our ability to protect the public from criminal threats is rapidly deteriorating. The status quo is exceptionally dangerous, unacceptable, and only getting worse. It is time for us to stop debating whether to address it, and start talking about how to address it.

My colleagues in the Department of Commerce will be reaching out to you soon to continue this dialogue. Please accept that invitation. And let's do more than just talk. Let's move forward in a good faith effort to find solutions.

#

AG

19-1070

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

Follow us:    

This email was sent to cyrus.farivar@nbcuni.com using GovDelivery, on behalf of [U.S. Department of Justice Office of Public Affairs](#) · 950 Pennsylvania Ave., NW · Washington, DC 20530 · 202-514-2007 · TTY (866) 544-5309. GovDelivery may not use your subscription information for any other purposes. [Click here to unsubscribe](#).

[Department of Justice Privacy Policy](#) | [GovDelivery Privacy Policy](#)